Security Architecture Work Group

Tuesday August 28, 2001
1:30 p.m. to 3:00 p.m.
Lincoln – Energy Square 1111 O Street, Room 112A
Kearney – UNK, 1918 University Drive Communications Building Room 250
Wayne State College

Minutes

A. Participants

Margo	Gamet	HHSS
Jerry	Hielen	IMServices
Sandy	LaLonde	IMServices
Dennis	Linster	Wayne State College
Scott	McFall	Nebraska State Patrol
George	McMullin	NECERT
Mike	Overton	Crime Commission
Leona	Roach	University of Nebraska
Steve	Schafer	Nebraska CIO
Gary	Wieman	Legislative Council

B. Security Procedures Documentation

Jerry Hielen and Sandy LeLonde reviewed the three draft documents:

- Security Officer Guide
- IS Department Template
- General Employee (User) Template

Sandy sought advise on several questions, options for training, and the section on business impact analysis. Discussion included the following points:

- The handbooks provide a wealth of specific material that security officers can choose from in tailoring procedures for their organizations. Although the Technical Panel and NITC will be asked to endorse the handbooks, the purpose of their action will be to encourage agencies and institutions to use the handbooks. It will not constrain the ability of agencies and institutions to modify the content to serve unique situations.
- The CIO / NITC will retain "ownership" of the templates and will sponsor periodic updates, using the Security Work Group as a forum.
- Training will be a major undertaking. Jerry Hielen distributed a training outline. IMServices can provide a two to four hour training session for agency security officers, but does not have the resources to offer training to other agency personnel. This training would be the first step in an overall awareness program. It would begin after the Technical Panel review and comment process and NITC endorsement (which could occur at their October 31 meeting). The training outline shows the amount and type of training IMServices plans to provide its own staff and contractors. The feasibility of computer-based training was discussed as an option.
- The handbooks still do not address the needs of very small agencies, which do not have the staff or skills to develop security programs, even with the aid of the handbooks.

- Enforcement in whether agencies use the handbooks or develop security programs that are consistent with NITC policies is an unresolved issue. Lack of authority and resources to create a "police" function are important constraints. As a practical matter, progress will largely depend on voluntary implementation. The next round of agency comprehensive information technology plans will include some questions regarding security as a way to increase awareness among agencies.
- The outline for conducting a business impact analysis generated considerable discussion because of concern about the time and effort it would take to go through the exercise of valuing all information assets (hardware, software, communications, and data). The purpose for conducting a business impact analysis is to develop a business case for security and help to determine a balance between cost of security and potential damages from security problems.

Steve Schafer asked whether the templates would be useful for agencies that are developing security plans and programs. The response from those attending the meeting was positive. He asked whether he should take the handbooks to the Technical Panel for their consideration. There was general agreement to move these forward.

C. Incident Reporting

Sgt. Christensen of the State Patrol was not able to attend this meeting. He is the official point of contact for reporting any computer crimes or suspicions of computer crimes. He will try to be at the September meeting. Scott McFall distributed Sgt. Christensen's business card. Contact information includes:

Sergeant Scott Christensen
Nebraska State Patrol, Internet Crimes Against Children Unit
4411 So. 108th Street
Omaha, Nebraska 68137
Phone: 402-595-2410; 24 Hr. Phone: 402-331-3333
Fax: 402-697-1409
Pager: 402-299-2088
e-mail: schriste@nsp.state.ne.us

Below is general information about gathering information, which Scott suggested should be added to the minutes:

Gathering information

To ensure that your organization can react to an incident efficiently, make sure that staff knows who is responsible for cyber security and how to reach them. The following steps will help you document an incident and assist federal, state, and local law enforcement agencies in their investigation (be sure to act in accordance with your organization's polices and procedures):

1. Encourage intrusion detection procedures;
2. Preserve the state of the computer at the time of the incident by making a backup copy of logs, damaged or altered files, and files left by the intruder;
3. If the incident is in progress, activate auditing software and consider implementing a keystroke-monitoring program if the system log on the warning banner permits;
4. Document all losses your organization suffered as a result of the incident. These could include:

- Estimated number of hours spent in response and recovery. (Multiply the number of participating staff by their hourly rates.)
- Cost of temporary help
- Cost of damaged equipment value of data lost
- Amount of credit given to customers because of the inconvenience
- Loss of revenue
- Value of any "trade secret" information

5. Contact law enforcement and provide incident documentation:
   - Share information about the intruder
   - Share any ideas about possible motives
   - Contact Information: To initiate an investigation, contact Sgt Scott Christensen, Nebraska State Patrol - Omaha. 402-595-2410 (24 hour dispatch) 402-331-3333

D. Other Implementation Issues

Steve Schafer announced that he and Steve Henderson are trying to organize a fall security forum on the topic of "perimeter security." The forum would include an outside expert, presentation by state staff, and a discussion of network security problems and issues that IMServices is trying to address. No date has been set.

E. Next Meeting Date

The meeting adjourned without setting a date. The agenda will include:

- Discussion of incident reporting
- Update on other security initiatives
- Discussion of other implementation options.